

Notice of Allowability

Application No.

10/631,023

Applicant(s)

EVANS ET AL.

Examiner

Nadia Khoshnoodi

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to interview conducted 7/30/2007.

2. The allowed claim(s) is/are 1, 3-26, 28-34, 36-94.

3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some* c) None of the:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. _____.

3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

(a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) hereto or 2) to Paper No./Mail Date _____.

(b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of
Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)

2. Notice of Draftsperson's Patent Drawing Review (PTO-948)

3. Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 3/5-24-2007

4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. Notice of Informal Patent Application

6. Interview Summary (PTO-413),
Paper No./Mail Date attached.

7. Examiner's Amendment/Comment

8. Examiner's Statement of Reasons for Allowance

9. Other _____.


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/2/2007 has been entered.

Response to Amendments

Claims 2, 27, and 35 have been cancelled. Applicant's arguments/amendments filed 8/2/2007 with regards to claims 1, 12, 23, 31, 39, 45, 53, 55, 70, and 87 have been fully considered and are persuasive. The previous rejection has been withdrawn.

EXAMINER'S AMENDMENT

An Examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's amendment was given in a telephone interview with Mr. Dan McGinnity, telephone no. (509) 755-7257, on August 2, 2007.

Please amend the application as follows:

Claims 39, 45, 53, 70, and 87 should be amended to the claim language as shown below.

All other claims, i.e. subsequent dependent claims not specifically mentioned are acceptable as filed on 8/2/2007.

These amendments to the claims will **replace** claim 39 as filed on 8/2/2007:

In the claims filed 8/2/2007, claim 39 **has been changed to --** 39. A system comprising:

means residing on a graphics processor unit (GPU) for decrypting, on a per cache page basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by the graphics processor unit (GPU) that resides on the video card and is separate from the cryptographic processor;

means for performing an operation on the decrypted data to provide resultant data;

means residing on the graphics processor unit (GPU) for re-encrypting, on a per cache page basis, the resultant data;

means for writing the encrypted resultant data to a video card memory surface associated with the video card, and a trusted software component to establish the one or more memory surfaces on the video card and negotiate one or more keys with the cryptographic processor such that each of the one or more memory surfaces is associated with at least one unique key; wherein the cryptographic processor distributes the one or more keys to said means for decrypting and said means for re-encrypting to perform the decrypting and re-encrypting respectively.--

These amendments to the claims will **replace** claim 45 as filed on 8/2/2007:

In the claims filed 8/2/2007, claim 45 **has been changed to --** 45. A system comprising: a video card;

a graphics processor unit (GPU) on the video card and configured to process video data

that is to be rendered on a display device;

memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card, separate from the GPU, and configured to initialize cryptographic hardware of the GPU including one or more encryptors and one or more decryptors to control encryption and decryption on the video card, the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted, on a per cache page basis by decryption hardware inside the GPU, in connection with an operation that is to be performed on the data by the GPU; and

a trusted software component to negotiate one or more keys with the cryptographic processor such that each of the one or more input and output memory surfaces is associated with at least one unique key, the cryptographic processor further being configured to distribute said negotiated keys to the cryptographic hardware of the GPU to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis by said one or more encryptors of the GPU, to an output memory surface.--

These amendments to the claims will **replace** claim 53 as filed on 8/2/2007:

In the claims filed 8/2/2007, claim 53 **has been changed to -- 53**. A method comprising: providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card; associating, with each input memory surface, a decryptor of the GPU that is uniquely

configured so as to decrypt the encrypted data that is held by the associated input memory surface;

decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to an output memory surface associated with the video card; wherein the video card includes a cryptographic processor as a distinct component separate from the GPU that is configured to: negotiate one or more cryptographic keys with a trusted software component; and initialize said decryptor of the GPU to perform said act of decrypting,

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.--

These amendments to the claims will **replace** claim 70 as filed on 8/2/2007:

In the claims filed 8/2/2007, claim 70 **has been changed to -- 70**. A method comprising:
providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;
associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface;
decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data; re-encrypting the resultant data; and writing the encrypted resultant data to an output memory surface associated with the video card, wherein the video card includes a cryptographic processor as a distinct component separate from the GPU that is configured to: negotiate one or more cryptographic keys with a trusted software component to associate each of the one or more memory surfaces with at least one unique key; and

initialize said decryptor of the GPU to perform said act of decrypting using the keys, said acts of decrypting and re-encrypting taking place on a per cache page basis.--

These amendments to the claims will **replace** claim 87 as filed on 8/2/2007:

In the claims filed 8/2/2007, claim 87 **has been changed to -- 87**. A system comprising:
a video card;
a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device; memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card and configured to control encryption and decryption on the video card, the cryptographic processor being separate from the GPU and comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card, said managing keys including:

negotiating the keys with a trusted software component such that each individual input memory surface has its own unique associated key for decrypting encrypted data held thereon; distributing corresponding keys to the GPU to enable encrypted data on one or more of the input memory surfaces to be decrypted by the GPU on a per cache page basis so that the decrypted data can be operated upon by the GPU; and distributing corresponding keys to the GPU to enable data that has been operated upon by the GPU to be encrypted on a per cache page basis to an output memory surface.--

Allowable Subject Matter

Claims 1, 3-26, 28-34, and 36-94 are allowed.

The following is an examiner's statement of reasons for allowance: The above mentioned claims are allowable over the prior arts because the CPA (Cited Prior Arts) of record taken singly or in combination fail to anticipate or render obvious the specific added limitations, as recited in all independent claims and subsequent dependent claims.

The CPA does not teach or suggest a method/system which comprises a GPU and a separate cryptographic processor which reside on a video card where a trusted component establishes at least one unique key with the cryptographic processor to associate each of the memory surfaces on the video card with the unique key.

Wong et al. (US Pub. No. 2003/0093683) teaches the use of a GPU which contains cryptographic capabilities used to encrypt/decrypt data before rendering/performing operations on the data by the GPU. However, Wong et al. fail to teach/suggest having a GPU and a separate cryptographic processor on the video card where a trusted component establishes at least one

unique key with the cryptographic processor to associate each of the memory surfaces on the video card with the unique key.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Nadia Khoshnoodi
Examiner
Art Unit 2137
8/3/2007

NK

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER